TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. 67539/00388

In Re Application Of: **POELUEV, Yuri**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/903,991	July 13, 2001	EL CHANTI, Hussein A.	27871	2157	2243

Invention: **METHOD AND APPARATUS FOR RESOLVING A WEB SITE ADDRESS WHEN CONNECTED WITH A VIRTUAL PRIVATE NETWORK (VPN)**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:

The fee for filing this Appeal Brief is: **$500.00**

□ A check in the amount of the fee is enclosed.

□ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 02-2553. I have enclosed a duplicate copy of this sheet.

□ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **June 20, 2007**

Brett J. Slaney (Reg. No. 58,772)
Blake, Cassels & Graydon LLP
Box 25, Commerce Court West, 199 Bay Street
Toronto, Ontario, M5L 1A9, Canada

Tel: (416) 863-2518
Fax: (416) 863-2653

I hereby certify that this correspondenceis being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed t"Commissioner for Patents, P.O. Box 1450, Alexandria,VA 22313-1450" [37 CFR 1.8(a)] on

______________.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appl. No.:	**09/903,991**
Applicant:	**POELUEV, Yuri**
Filed:	**July 13, 2001**
Title:	**METHOD AND APPARATUS FOR RESOLVING A WEB SITE ADDRESS WHEN CONNECTED WITH A VIRTUAL PRIVATE NETWORK (VPN)**
Art Unit:	**2157**
Examiner:	**EL CHANTI, Hussein A.**
Docket No.:	**67539/00388**

Board of Patent Appeals and Interferences
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
USA

BRIEF ON APPEAL

This is an appeal of the Final Office Action of the Examiner dated January 24, 2007. A Notice of Appeal from the Primary Examiner to the Board of Patent Appeals and Interferences was timely filed with the Office on April 20, 2007.

REAL PARTY IN INTEREST:

The real party in interest in the present application is Certicom Corp. The assignment from the Applicant to Certicom Corp. was registered with the office on reel/frame 012244/0996 on October 12, 2001.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals or interferences known to the Appellant, Appellant's representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS:

In this application, claims 1, 4 and 12-19 are pending. Claims 1, 4 and 12-19 have been finally rejected and are being appealed. Please refer to the Claims Appendix for a complete listing of the claims.

STATUS OF AMENDMENTS:

A response to the office action dated October 4, 2004 was filed on April 4, 2005, wherein claims 2, 3 and 5 were cancelled and claims 12-19 were added.

The above amendments were entered by the Examiner as indicated in the final office action dated June 22, 2005. A response after final rejection was filed on October 24, 2005, with clarifying amendments to claim 1, along with a request for continued examination.

A non-final rejection was issued on January 13, 2006, to which a response was filed on June 28, 2006, in which the claims were amended to clarify the nature of steps recited.

The above amendments were entered by the Examiner, as indicated in the final office action dated September 8, 2006. Further arguments were presented in a response dated November 7, 2006 and no further amendments were made.

An advisory action issued on December 6, 2006 indicating that the application was not in condition for allowance and a request for continued examination was filed on the same day.

A final office action was then issued on January 24, 2007, which forms the basis for the present appeal.

A Notice of Appeal from the Primary Examiner to The Board of Patent Appeals and Interferences was then filed on April 20, 2007. Appellant notes that no amendments have been filed subsequent to the final action dated January 24, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER:

In one aspect (claims 1, 4 and 12-16) a method for transparently resolving a web site address (e.g. www.certicom.com see page 4, lines 10-12) for a public host (e.g. host A, numeral 20, see Figure 1) in a public network (e.g. public network 12 see Figure 1) is provided for when the public host (20) is connected to a virtual private network (VPN) (e.g. VPN 14, see Figure 1 and page 3, lines 26-30).

The method comprises connecting the public host (20) with a VPN (14), the public host (20) having a software module included therein for routing domain name requests to a domain name server of the VPN while the connection is active, the software module operating transparent to the user (see page 5, lines 15-24). The software module monitors communication packets transmitted from the public host (20) for the presence of domain name requests outbound from the public host (20) and transparently intercepts the requests (see page 5, lines 22-23 and step 30, Figure 2).

The software module then modifies the requests (see page 5, lines 25-26, and step 32 in Figure 2) by replacing an address of a DNS (18) of an ISP (16) (see Figure 1) of the public host (20) with the address of the DNS of the VPN (see page 5, lines 26-27 and numeral 26 in Figure 1) and routing the requests to the DNS of the VPN (26) (see step 34, Figure 2). The DNS of the VPN (26) resolves the requests routed thereto by the software module (see page 6, lines 14-15 and step 36, Figure 2) and returns an address location to the software module as a domain name response (see step 40, Figure 2 and page 6, lines 17-18). The software module then modifies the response by re-modifying the address of the ISP to counter-act the IP address modification previously performed (see page 6, lines 20-21) and the software module provides the address location to the public host (see page 6, lines 22-24). The address location appears to the public host (20) as being provided by the DNS of the ISP (see page 6, line 21).

In another aspect (claims 17-19), a system for transparently resolving a web site address for a public host (20) in a public network (12) is provided for when the public host (20) is connected to a VPN (14) The system comprises a domain name server (DNS) of the VPN (26) for resolving domain name requests from the public host (20) and for returning an address location as a domain name response. The system also comprises a software module that operates as discussed above and thus the details thereof need not be reiterated. The system also comprises a communication link (e.g. VPN tunnel seen in Figure 1) between the software module and the DNS of said VPN (26) for transmitting the request and the response;

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Claims 1, 4 and 12-19 are pending in this application and do not stand allowed.

The Appellant wishes to have the following ground(s) of rejection to be reviewed on appeal:

- Claims 1, 4 and 12-19 being finally rejected by the Examiner under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,832,322 to Boden ("Boden" hereinafter).

The Appellant respectfully traverses the Examiner's rejections.

APPELLANT'S ARGUMENTS:

Statement of the Law Regarding 35 U.S.C. 102(e):

According to 35 U.S.C. 102(e)(2): "A person shall be entitled to a patent unless – … (e) the invention was described in - …(2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent…".

As set forth in MPEP 2131, to anticipate a claim, the reference must teach each and every element of the claim.

What Claim 1 Recites:

Claim 1 is directed to a method for transparently resolving a web site address for a <u>public host</u> in a public network when the public host is connected to a virtual private network (VPN). The method comprises, in part, the following steps:

> a) connecting said public host with a virtual private network (VPN), said public host having a software module included therein for routing domain name requests to a domain name server (DNS) of said VPN while said connection is active, said software module operating transparent to said public host;

b) said software module monitoring communication packets transmitted from said public host for the presence of domain name requests outbound from said public host;

c) said software module transparently intercepting said requests;

It is believed to be clear from these steps that the public host has a software module included therein (i.e. the software module is at the public host), and that the software module operates transparently to the public host. As recited in claim 1, the software module also routes domain name requests while the connection is active by monitoring and intercepting the requests. Accordingly, the software module operates only when the connection to the VPN is active without the public host being aware. Also, when the VPN connection is not active, since the software module does not intercept packets, inherently, the public host operates as per the usual.

What Boden Teaches

Boden teaches a network address translation (NAT) scheme that intends to avoid IP address collisions while solving the problem of distributing common information, without multiple copies and the problems associated with maintaining currency of multiple copies (see col. 7, lines 64-67). To achieve this, Boden incorporates NAT with IPSec at the gateway nodes (see col. 5, lines 19-21) wherein user configured NAT rules are implemented and kept current at the gateway. Figure 2 of Boden clearly shows a host 474 that connects to an external host 476, through a VPN gateway 470 at their end and in turn a VPN gateway 472 at the external host's end. Also evident from Figure 2 of Boden is that the DNS 468 associated with VPN gateway 470 references a logical information table 469, and the VPN gateway 470 accesses a mapping table 480. Since Boden intends on running the NAT to avoid IP address collisions with respect to the hosts 474, 476, it can be understood that, once configured, the VPN gateway 470 is required to always intercept packets, regardless of whether the host 474 is attempting to connect with a VPN or any other node in the network. In any event, Boden does not teach or suggest incorporating a software module at the host but rather includes a mapping table at the gateway.

Examiner's Interpretation

Applicant believes that the Examiner has improperly interpreted the terminology in both claim 1 and the teachings in Boden in finding an equivalent to the software module recited in claim 1.

In particular, the Examiner states, in the Advisory Action dated December 6, 2006, that: "Boden teaches a system including a VPN gateway 470 'public host' receives intercepting packets from Network A 462 'VPN'"; and "Therefore , Boden teaches a VPN gateway 'public host' intercepting packets". Accordingly, it appears that the Examiner has in fact equated a gateway in Boden with the public host recited in claim 1. The reason for this interpretation appears to be on the basis that: "the claims must be given their broadest reasonable interpretation", as stated in the Advisory Action.

Remarks Regarding Examiner's Interpretation

Applicant believes that the Examiner has gone too far in equating a gateway to a public host. The terms 'gateway' and 'host' are well understood and are actually included in industry standard definitions. The Evidence Appendix includes such definitions as extracted from the Federal Standard 1037C (available at: http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm). A host and a gateway are not interchangeable and are well understood to be different entities that perform different tasks in a communications network. A host is the collection of hardware and software that makes use of a packet to support user to user or end to end communications, whereas, a gateway is a network node equipped for interfacing with another network that uses different protocols.

Discussion of How Claim 1 Distinguishes over Boden:

It is believed that Boden clearly adheres to the definitions and industry accepted terminology for defining a gateway. In fact, at col. 5, lines 21-21, Boden refers to a definition for "IP Sec gateway" in RFC2401. Moreover, Boden even shows a separate host 474 and gateway 470. There is no doubt in reading Boden that the gateway is not a host but rather a gateway as understood in the field of network communications. Appellant therefore respectfully submits that a person skilled in the art would not consider a gateway as taught in Boden as being equivalent or even have features applicable to a public host.

As noted above, claim 1 explicitly recites having a software module included in the public host monitor and intercept packets. This enables the public host to be able to connect to a VPN without having parameters reconfigured. The solution provided by the method recited in claim 1 solves a particular problem, namely where parameters of the public host are not alterable but need to be to access a VPN, which is not addressed, let alone solved by Boden. Boden is concerned with avoiding IP collisions by performing NAT at the gateway. This is not the same problem and Boden provides an entirely different solution. Boden does not provide a software module at the host and thus does not achieve the same effect as the method recited in claim 1, namely "wherein said address location appears to said public host as being provided by said DNS of said ISP".

Even if, for the sake of argument, one were to consider the 'gateway' in Boden as a 'public host' (which is entirely unlikely), there is no discussion of utilizing a software module that is to be operable when a connection is active. In fact, Boden does not discuss any modules or features within the gateway that operate as recited in claim 1. As outlined above, claim 1 clearly recites that the software module routes domain name requests when the connection is active. In Boden, it can only be inferred that the gateway is required to perform NAT for all routing and thus if Boden were to include the software module recited in claim 1 as suggested by the Examiner, the gateway would not work without making undisclosed modifications. Again, the Examiner has not shown that the gateway operates by providing a separate software module therein, let alone as recited in claim 1.

The Examiner has not shown where Boden teaches providing a software module at the gateway and rather seems to equate the entire gateway to the software module. If this is the case, then the gateway would be inoperable unless the host is requesting to connect to a VPN. Given that a gateway is an access node, this is contradictory to the purpose of a gateway. A gateway is inherently placed between the public host and another network and thus a gateway operates further down the system than the public host and thus cannot be considered to operate in the same way. It is believed that the Examiner's interpretation is improper and appears to be based on hindsight, since there is no reason that a person skilled in the art would consider a gateway to be equivalent to a public host having a software module. The Examiner appears to have first looked at claim 1 and then asserted that certain passages in Boden equate to the steps in claim 1, without fully considering how the operation of such steps would be understood by a person skilled in the art in the context of what is recited in claim 1. As such, Boden clearly does not teach what is recited in claim 1 and a person skilled in the art would not consider the gateway in Boden as being equivalent to the public host with software module therein, recited in claim 1.

Accordingly, Boden does not teach providing a software module included in the public host for routing domain name requests while the VPN connection is active and thus cannot anticipate claim 1. Claims 4 and 12-16, being ultimately dependent on claim 1 are also believed to be distinguished with respect to Boden.

Claim 17 is directed to a system for transparently resolving a web site address for a public host in a public network when said public host is connected to a virtual private (VPN) and comprises a software module that operates as discussed above. As such, the above arguments equally apply to claim 17. Claims 18-19 being dependent on claim 17 are also believed to be distinguished.

CONCLUSION:

In view of the foregoing, the Appellant believes that Boden does not teach every element recited in claims 1, 4 and 12-19 and thus cannot anticipate. Accordingly, the Appellant believes that the Examiner has erred in rejecting claims 1, 4 and 12-19 under 35 U.S.C. 102(e).

The Appellant respectfully requests that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the allowability of all pending claims in this application, namely claims 1, 4 and 12-19.

Respectfully submitted,

Date: June 20/07

Brett J. Slaney
Agent for Applicant
Registration No. 58,772

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA
BSL/

Tel: 416.863.2518

CLAIMS APPENDIX:

Listing of the claims involved in the appeal:

1. (previously presented) A method for transparently resolving a web site address for a public host in a public network when said public host is connected to a virtual private network (VPN), said method comprising the steps of:

a) connecting said public host with a virtual private network (VPN), said public host having a software module included therein for routing domain name requests to a domain name server (DNS) of said VPN while said connection is active, said software module operating transparent to said public host;

b) said software module monitoring communication packets transmitted from said public host for the presence of domain name requests outbound from said public host;

c) said software module transparently intercepting said requests;

d) said software module modifying said requests by replacing an address of a DNS of an internet service provider (ISP) of said public host with the address of said DNS of said VPN and routing said requests to said DNS of said VPN;

e) said DNS of said VPN resolving said requests routed thereto by said software module and returning an address location to said software module as a domain name response;

f) said software module modifying said response by re-modifying said address of said ISP to counter-act the IP address modification performed in step d); and

g) said software module providing said address location to said public host;

wherein said address location appears to said public host as being provided by said DNS of said ISP.

2. – 3. (canceled)

4. (previously presented) The method of Claim 1 further including the step of connecting said host to said address location.

5 – 11. (canceled)

12. (previously presented) The method of Claim 1, wherein step d) further comprises said software module modifying a check sum of said domain name requests; and step f) further comprises said software module re-modifying said check sum to counter-act the original check sum modification performed in step d).

13. (previously presented) The method of Claim 12, wherein said modification of said check sum includes computing a new check sum by XORing said check sum with a hexadecimal value to obtain a one's complement, and replacing said check sum with said new check sum.

14. (previously presented) The method of Claim 1, wherein said connection between said public host and said VPN is a VPN tunnel.

15. (previously presented) The method of Claim 14, wherein said VPN tunnel is a Secure Internet Protocol (IPSec) tunnel.

16. (previously presented) The method of Claim 1, wherein said public host is one of a personal digital assistant (PDA), a desktop personal computer, and a laptop personal computer; having data communication capabilities.

17. (previously presented) A system for transparently resolving a web site address for a public host in a public network when said public host is connected to a virtual private (VPN), said system comprising:

a domain name server (DNS) of said VPN for resolving domain name requests from said public host and for returning an address location as a domain name response;

a software module transparently included in said public host for monitoring communication packets outbound of said public host for the presence of said domain name requests; for transparently intercepting said requests; for modifying said requests by replacing an address of a DNS of an internet service provider (ISP) of said public host with an address of said DNS of said VPN and routing said requests to said DNS of said VPN; for receiving said response and modifying said response from said DNS of said VPN by re-modifying said address of said ISP to counter-act the address modification performed on said request; and for providing said address location to said public host; and

a communication link between said software module and said DNS of said VPN for transmitting said request and said response;

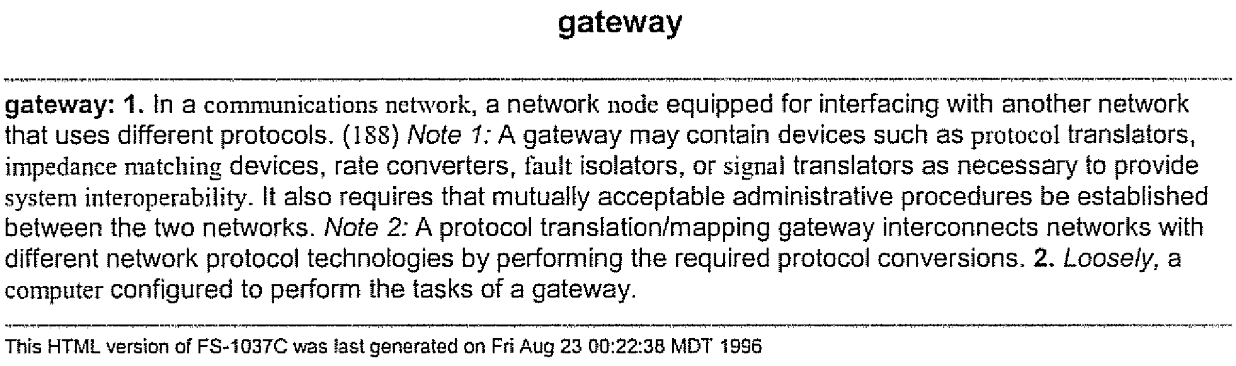
wherein said address location appears to said public host as being provided by said DNS of said ISP.

18. (previously presented) The system of Claim 17, wherein said software module is a driver.

19. (previously presented)The system of Claim 17, wherein said public host is one of a personal digital assistant (PDA), a desktop personal computer, and a laptop personal computer; having data communication capabilities compatible with said communication link.

EVIDENCE APPENDIX:

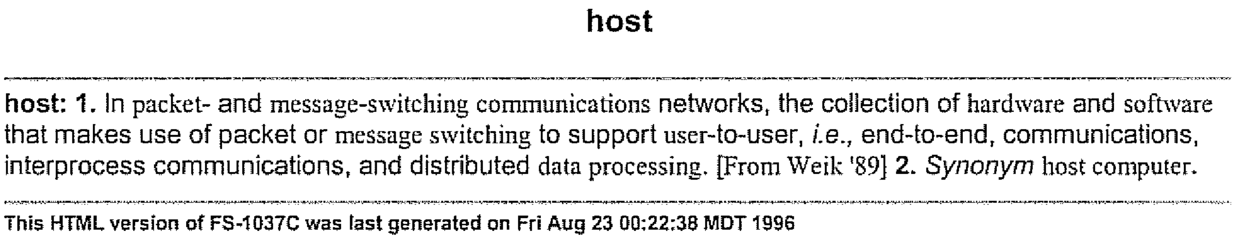
Accessed from online records of Federal Standard 1037C on June 18, 2007. Website available at: **http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm**



gateway

gateway: 1. In a communications network, a network node equipped for interfacing with another network that uses different protocols. (188) *Note 1:* A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires that mutually acceptable administrative procedures be established between the two networks. *Note 2:* A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions. **2.** *Loosely,* a computer configured to perform the tasks of a gateway.

This HTML version of FS-1037C was last generated on Fri Aug 23 00:22:38 MDT 1996



host

host: 1. In packet- and message-switching communications networks, the collection of hardware and software that makes use of packet or message switching to support user-to-user, *i.e.*, end-to-end, communications, interprocess communications, and distributed data processing. [From Weik '89] **2.** *Synonym* host computer.

This HTML version of FS-1037C was last generated on Fri Aug 23 00:22:38 MDT 1996

RELATED PROCEEDINGS APPENDIX:

[None]